

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

ROBERT ALPERT, *et al.*

§

Plaintiffs,

§

v.

§ CIVIL ACTION NO. H-04-3774

MARK R. RILEY, *et al.*

§

Defendant.

§

MEMORANDUM AND ORDER

This case involves allegations that Mark Riley improperly exercised the authority of a trustee over trusts created by Robert Alpert and improperly exercised the authority of an attorney and agent over other aspects of Alpert's business and financial affairs. Riley, Alpert, and the trust beneficiaries are also litigants in a probate court suit involving some of the same trusts at issue in this case. Riley is represented by counsel in this case and by separate counsel in the probate court litigation. Riley objected to some of the discovery requests in this case on the ground that the documents sought are subject to attorney-client privilege and work-product protection. Alpert and the trust beneficiaries responded that Riley waived the privilege and protection as to documents he placed on a computer belonging to a third party—who was adverse to Riley in separate litigation—and left in the possession of that third party even after that litigation ended in a settlement. On February 9, 2010, this court held an evidentiary hearing to determine whether Riley had waived attorney-client privilege and work-product protection as to those documents. After the evidentiary hearing, the parties filed briefs on the issue.

Based on the evidence, the record, the parties' submissions, the arguments of counsel, and the applicable law, this court holds that Riley waived any attorney-client privilege and work-product protection in the materials he had placed and left on Robert Hux's computer. The reasons are explained below.

I. The Record

Mark Riley and Robert Hux testified at the February 9, 2010 hearing. In October 1998, Mark Riley moved into offices leased by Robert Hux on St. James Place in Houston. Hux, a certified public accountant, and Riley, an attorney and businessperson, knew each other through attending sporting events. In the fall of 1998, they were partners in a company called RRAM Investments LLC. According to Hux, Riley and his legal assistant, Dixie Meynier, arrived at Hux's offices uninvited, but Hux allowed them to use the offices because he was involved in a partnership with Riley. According to Riley, the move had been arranged. It is undisputed that Riley did not pay rent at the St. James location and the lease was in Hux's name. Riley and Hux used the offices for matters relating to their joint business in RRAM Investments LLC. Both also used the offices for other, separate business activities.

In early 2000, Riley and Hux moved to offices in the nearby Marathon office building. The rent on the Marathon office space was split between RRAM and several trusts for which Hux served as trustee. Riley signed the lease on behalf of RRAM but Hux paid all the rent and office expenses. When Hux and Riley moved to the Marathon office space, Hux brought a new computer for his own use at the office. Riley brought his own laptop and a computer he owned that Meynier used, as well as a network drive he owned. Riley set up all of the computers in the Marathon office on a network. The network included Riley's personal laptop and Meynier's computer, as well as the new computer

Hux had purchased, another computer owned by Hux and used by his assistant, Ginger Parks, and an old computer that Hux owned and that was used for a period by RRAM staff members.¹

Around the same time, Riley made a copy of a directory on his laptop named “Legal.” Riley placed the copy of this directory on the C:/ drive of Hux’s old computer that was then being used by RRAM staff members. Riley did not advise anyone that he had done this. The directory, unrelated to RRAM, contains the documents at issue in this case.

Riley made himself the network administrator for the computers in the Marathon office suite. Riley set up custom login names with passwords for each user on the network. Riley also regulated which drives and directories could be accessed by which users. Riley had a personal user login that enabled him to view his and Meynier’s drives. He also had an administrator login that gave him access to all the computers on the network. There is no evidence that Riley shared this login with anyone. Meynier’s login gave her access to her own computer only. Hux’s and Parks’s logins did not allow them to access Riley’s or Meynier’s computers or Hux’s old computer. Two or three RRAM employees worked at Hux’s old computer and were given logins that allowed them to do so. No one but Riley knew about or could access Riley’s “Legal” directory on Hux’s old computer. Only Riley had access to that directory, although it is unclear whether he had this access through his personal login or through his administrator login.

Riley also installed an application called “Driveway” on Hux’s old computer. This application was used to backup RRAM files on the network drive to an online storage space that in turn enabled remote access to the stored information. The Driveway software was not used to backup the “Legal” directory.

¹ There is some evidence in the record that other individuals also worked in both the St. James and Marathon office space. It is unclear whether their computers were part of the network Riley created.

In May 2001, Riley and Hux were involved in forming a new limited liability company called Hospital Systems Solutions (“HSS”). The company was run out of the Marathon office suite. Sometime later that year, a dispute arose between Riley and Hux about HSS’s ownership. On advice of counsel, Hux locked Riley out of the Marathon office suite. A short time later, Riley and Hux met with Hux’s attorneys. They agreed that Riley would leave the office suite and that Hux would return to Riley all the computers and computer equipment that Riley owned, with his paper files and other belongings.

Riley’s computers and related equipment were returned two weeks after that meeting. During those two weeks, Hux arranged to have the data stored on Riley’s laptop copied. The data copied did not include the Legal directory stored on Hux’s computer; no one but Riley knew that he had files stored on that computer and no one but Riley had access to that directory. Hux later gave the copies of data from Riley’s laptop to his attorneys at Gibbs & Bruns LLP. When the computers Riley owned—his laptop, Meynier’s computer, and the network drive—were returned to him, the logins and passwords had been either been disabled or changed. Riley reset them, using new logins and passwords that allowed him to access the data he had stored on those computers. Riley did not ask about the directory he had placed on Hux’s old computer or tell anyone involved with Hux about that directory. At that time, Riley was not aware that Hux had copied the data from Riley’s laptop before returning it.

Within three weeks of the lockout, Riley sued Hux, alleging that he had improperly transferred customer lists and other information Riley had developed for HSS to another company Hux owned and with which Riley was not involved. Hux countersued. The parties asked for and the state court entered a protective order in that litigation. (Evidentiary Hearing Ex. 1). Under the

protective order, documents and information that the parties exchanged in discovery that they designated as confidential could not be disclosed to third parties except under limited circumstances. (*Id.* at 3-4). On June 1, 2002, Hux and Riley reached an agreement to settle the lawsuit. (Evidentiary Hearing Ex. 2). The Settlement Agreement contained the following provisions:

The Hux Parties agree that all materials and data copied from Mark Riley's computer have been delivered to Gibbs & Bruns and have been designated as Confidential Discovery Material as that term is defined in the Protective Order in the Consolidated Suit and shall be fully subject to the Protective Order as if it had been initially so designated.

...

Survival of Agreements. All representations and warranties of the Company and Riley Parties herein, and all covenants and agreements herein not fully performed before the Effective Date of this Settlement Agreement, shall survive such date.

(*Id.* at 9, 16). During and after that litigation, Riley did not tell anyone that he had stored a directory entitled "Legal" on Hux's computer. Nor did Riley ask for this data to be returned.

In 2004, Hux took his old computer—on which Riley had placed the "Legal" directory—home for personal use. When Hux began using the computer, an error message appeared. Hux asked an employee knowledgeable about information technology, Jason Brodman, to come to the house to help with the problem. Brodman testified in the evidentiary hearing that the error message related to the Driveway software that Riley had installed on the computer. After Brodman uninstalled Driveway, he examined the computer to see if there were other problems. He found the "Legal" directory that Riley had backed up on the hard drive. Brodman could not recall if he needed a user name and password to log into Windows on the computer. But Brodman was certain that no separate password was required to gain access to the Legal directory or any of the folders or files within that directory.

Sometime later, Brodman returned to Hux's house and copied the "Legal" directory on to disks. Brodman kept those disks until he was contacted by Daniel Henderson, an employee of Robert Alpert. Henderson asked Brodman to describe the data, apparently to determine whether it matched data that was in Alpert's possession. Brodman then gave the disks to Ginger Parks, who worked for Hux. Hux was advised by the lawyers who had represented him in the Hospital Systems Solutions litigation against Riley that the Settlement Agreement in that case did not require him to turn over the data copied from Hux's old computer to Riley. In 2005, Riley learned that Hux had these disks and had given them to Alpert.

Alpert argues that Riley waived any attorney-client privilege or work-product protection in the "Legal" directory by placing that directory on Hux's computer and then failing to take any steps to retrieve the information even after he knew that the computer passwords had been disabled and that the information had not been returned to him. (Docket Entry No. 323 at 6). Riley argues that the data was initially password-protected and that the protective order and Settlement Agreement in the Hospital Systems Solutions litigation maintained the privileged status of the information, even after he knew that the passwords he had installed had been disabled and that the information remained on Hux's computer. These arguments are considered below.

II. The Applicable Law

Federal Rule of Evidence 501 provides:

Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law

supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.

FED.R.EVID. 501. Under Rule 501, “[q]uestions of privilege that arise in the course of adjudication of federal rights” are governed by the federal common law of attorney-client privilege. *Willy v. Administrative Review Bd.*, 423 F.3d 483, 495 (5th Cir. 2005) (quoting *United States v. Zolin*, 491 U.S. 554, 562, 109 S. Ct. 2619 (1989)). When state law provides the rule of decision, however, state privilege law applies. The plaintiffs in this case have alleged both federal- and state-law causes of action and the parties are completely diverse.

The information sought by the plaintiffs are relevant to both the federal- and state-law claims. In such a situation, some courts have found it appropriate to apply federal common law of attorney-client privilege and waiver. *Ferko v. National Ass’n for Stock Car Auto Racing, Inc.*, 218 F.R.D. 125, 134 (E.D. Tex. 2003) (“In cases where a federal question exists, the federal common law of attorney-client privilege applies even if complete diversity of citizenship is also present.”); *First Federal Sav. & Loan Ass’n v. Oppenheim, Appel, Dixon & Co*, 110 F.R.D. 557, 560 (S.D.N.Y. 1986) (“When evidence that is the subject of an asserted privilege is relevant to both federal and state law claims, the courts have consistently held that federal law governs the privilege.”); *see also In re Combustion, Inc.*, 161 F.R.D. 51, 53-54 (W.D. La. 1995) (“I further hold that the federal law of privilege provides the rule of decision with respect to privilege issues affecting the discoverability of evidence in this federal question case involving pendent state law claims.”). Neither the Supreme Court nor the Fifth Circuit has resolved this issue. The Supreme Court recognized the problem but declined to decide the appropriate rule. *See Jaffee v. Redmond*, 518 U.S. 1, 17 n. 15, 116 S. Ct. 1923 (1996) (declining to decide “the proper rule in cases . . . in which both federal and state claims are

asserted in federal court"). In this case, because the applicable federal and Texas state law of waiver are similar, there is no need to decide this issue.

The attorney-client privilege, when applicable, shields from disclosure confidential communications between an attorney and client. *See United States v. Neal*, 27 F.3d 1035 (5th Cir. 1994). The privilege fosters frank communication between attorneys and their clients:

The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law. Its purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.

Upjohn Co. v. United States, 449 U.S. 383, 389 (1981). Like other evidentiary privileges, the attorney-client privilege is based on statutory and common law. *See, e.g., Clutchette v. Rushen*, 770 F.2d 1469, 1471 (9th Cir. 1985), *cert. denied*, 475 U.S. 1089 (1986) ("Standing alone, the attorney-client privilege is merely a rule of evidence; it has not yet been held a constitutional right."). Under federal common law, a party asserting attorney-client privilege must establish "(1) that he made a confidential communication; (2) to a lawyer or his subordinate; (3) for the primary purpose of securing either a legal opinion or legal services, or assistance in some legal proceeding." *United States v. Robinson*, 121 F.3d 971, 974 (5th Cir. 1997). Texas Rule of Evidence 503 is similar. Under both federal common law and Texas Evidence Rule 503, the client, not the client's attorney, holds the privilege. *See In re Grand Jury Subpoenas*, 561 F.3d 408, 411 (5th Cir. 2009); TEX. R. EVID. 503(b)(1).

Federal Rule of Civil Procedure 26(b)(3) protects against the disclosure of work product, which is defined as "documents and tangible things that are prepared in anticipation of litigation or

for trial” that would otherwise disclose “the mental impressions, conclusions, opinions, or legal theories of a party’s attorney or other legal representative concerning the litigation.” A party resisting discovery based on work-product protection has the burden of establishing that 1) the materials at issue are documents or tangible things; 2) prepared in anticipation of litigation or for trial; 3) by or for a party’s representative; 4) that contains the mental impressions, conclusions, opinions, or legal theories of an attorney. *See Ferko*, 218 F.R.D. at 136 (citing 8 CHARLES A. WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2024, at 336 (2d ed. 1994)). Texas Rule of Civil Procedure 192.5 is similar, encompassing materials or communications “prepared or mental impressions developed in anticipation of litigation or for trial by or for a party or a party’s representatives, including the party’s attorneys, consultants, sureties, indemnitors, insurers, employers, or agents.” TEX. R. CIV. P. 192.5(a). Under federal and Texas law, work-product protection belongs to both the client and the attorney, either of whom may assert it. *See In re Grand Jury Subpoenas*, 561 F.3d at 411.

Under federal law, “voluntary disclosure of information which is inconsistent with the confidential nature of the attorney client relationship waives the privilege.” *Alldread v. City of Grenada*, 988 F.2d 1425, 1434 (5th Cir. 1993); *see Ratliff v. Davis Polk & Wardwell*, 354 F.3d 165, 170 (2d Cir. 2003) (documents sent to a law firm for legal advice were not protected on privilege grounds once the client voluntarily authorized the law firm to send those documents to the S.E.C.); *United States v. Mass. Inst. of Tech.*, 129 F.3d 681, 684–87 (1st Cir. 1997) (a government contractor’s disclosure of documents to the Defense Department’s audit agency waived attorney-client privilege with respect to those documents; privilege was not a defense to an IRS summons regarding those documents). Privilege may also be waived by inadvertently disclosing information.

Id. “The party asserting the attorney-client privilege must prove that the confidentiality of the communications have been preserved.” *United States v. Citgo Petroleum Corp.*, No. C-06-563, 2007 WL 1125792, at *2 (S.D. Tex. Apr. 16, 2007) (citing *United States v. El Paso Co.*, 682 F.2d 530, 539 (5th Cir. 1982)). Waiver is a fact-specific question that should be assessed on a case-by-case basis. *Allread*, 988 F.2d at 1434. Much of the case law concerning inadvertent disclosure developed in the context of privileged materials unintentionally produced to an opposing party during discovery. *See id.* at 1433-34 (citing *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323 (N.D. Cal. 1985); *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985)).

Waiver through disclosure in federal or state proceedings is addressed by Federal Rule of Evidence 502, which states in relevant part as follows:

(b) Inadvertent disclosure. — When made in a federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if:

- (1) the disclosure is inadvertent;
- (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
- (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

(c) Disclosure made in a state proceeding. — When the disclosure is made in a state proceeding and is not the subject of a State-court order concerning waiver, the disclosure does not operate as a waiver in a federal proceeding if the disclosure:

- (1) would not be a waiver under this rule if it had been made in a Federal proceeding; or

(2) is not a waiver under the law of the State where the disclosure occurred.

Rule 502(b) retains—without codifying—the multifactor test set out in the case law, which is “a set of non-determinative guidelines that vary from case to case.” FED. R. EVID. 502(b) Committee Note. The factors to consider include: “(1) the reasonableness of precautions taken to prevent disclosure; (2) the amount of time taken to remedy the error; (3) the scope of discovery; (4) the extent of the disclosure; and (5) the overriding issue of fairness.” *Alldread*, 988 F.2d at 1433-34 (citing *Hartford Fire Insurance*, 109 F.R.D. at 332); *see also In re Grand Jury (Impounded)*, 138 F.3d 978, 981 (3d Cir. 1998) (“In determining whether a party has waived the privilege through an inadvertent or involuntary disclosure, courts consider, among other factors, the steps taken by a party to remedy the disclosure and any delay in doing so.”). The Texas Supreme Court has adopted a similar standard. *Granada Corp. v. Honorable First Court of Appeals*, 844 S.W.2d 223, 226 (Tex. 1992).² This waiver analysis is identical for attorney-client privilege and work-product protection. *Bowles v. National Ass'n of Home Builders*, 224 F.R.D. 246, 257 n.15 (D.D.C. 2004).

III. Analysis

² After *Granada* was decided, Texas Rule of Civil Procedure 193.3(d) was enacted. This provision is similar to Federal Rule of Evidence 502 in restricting when inadvertent disclosure during discovery will waive the privilege. The Rule states:

A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if--within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made--the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

TEX. R. CIV. P. 193.3(d). Like Rule 502, this rule does not appear to govern the effect of disclosures that do not occur in discovery.

The disclosure at issue in this case did not occur in discovery in a court proceeding. Riley placed the information on Hux's computer in 1998, before any litigation had begun. Riley did not produce the information to Hux during discovery in the litigation between them. Rather, Hux discovered the information years after his lawsuit with Riley had ended. The waiver issue is not governed by Rule 502 or its Texas counterpart, but rather by common law.

The plaintiffs argue first that Riley voluntarily, rather than inadvertently, disclosed the "Legal" directory when he backed it up on Hux's computer. The record does not support this argument. When Riley placed the data on Hux's computer, he took steps to protect confidentiality. Although Hux owned the computer and none of the files or folders were password-protected, Riley was the network administrator and had set up the network such that only he had access to the "Legal" directory. Whether the directory was accessible through the administrator username and password only or also through Riley's personal username and password, Riley was the only person who could open the files. Riley did not tell anyone about the files or that they were confidential, but he took steps to deny access to other users on the network. During the time Riley was working at the Marathon office, that protected the confidentiality of the data. No privilege was waived when Riley put his information on Hux's computer.

After Riley was locked out of the office, however, he lost the ability to protect the confidentiality of the data he had placed on Hux's computer. Two weeks after the lockout, the computers Riley owned were returned with the passwords changed or disabled. This was a clear sign that someone had gained access to the office network. Riley's network drive was also returned, indicating that the network had been modified. Riley, who understood the network well enough to create and maintain it, would have understood that someone else had gained access at the

administrator level. The need for such an action was clear; Riley, who had been the network administrator with control over network permissions, was no longer working in the office. Riley knew that someone, likely a new administrator, had disabled the passwords on the two computers he received back from Hux. Riley knew, or reasonably should have known, that individuals in Hux's office now had access to the "Legal" directory he had placed on Hux's old computer as well. Riley does not dispute that he failed to notify Hux or anyone else about the confidential material on the hard drive and failed to ask for it to be deleted or returned.

The record does not support the plaintiffs' argument that Riley's failure to take any action to recover the "Legal" directory he had placed on Hux's computer after being locked out of the office was an intentional disclosure. There is no evidence that Riley intended to make the information on that directory available to Hux or others. Instead, the issue is appropriately addressed as one of inadvertent disclosure; whether, under the factors identified in the case law, Riley's failure to take action to retrieve the directory waived any privilege attached to the information it contained.

The first factor is the reasonableness of the steps taken to avoid disclosure. *Allread*, 988 F.2d at 1433-34 (citing *Hartford Fire Insurance*, 109 F.R.D. at 332). Riley argues that obtaining the protective order and Settlement Agreement in the Hospital Systems Solutions litigation protected the confidentiality of the directory and files and required their return. The plaintiffs argue that these documents do not apply to the directory and files Riley had placed on Hux's computer.

The protective order stated that any information designated as "Confidential Discovery Material" in the Hospital Systems Solutions litigation could not be used or disclosed by a nonproducing party outside the litigation without consent. The "Legal" directory was not disclosed in discovery in that litigation and was not designated as Confidential Discovery Material. Riley

argues that the Settlement Agreement extended the protective order to the files contained in the directory at issue. The Settlement Agreement was executed in 2002. It states in relevant part that “[t]he Hux Parties agree that all materials and data copied *from Mark Riley’s computer have been delivered* to Gibbs & Bruns and have been designated as Confidential Discovery Material as that term is defined in the Protective Order in the Consolidated Suit and shall be fully subject to the Protective Order as if it had been initially so designated.” (Evidentiary Hearing Ex. 2 at 9 (emphasis added)). By this provision, Hux confirmed that he had already returned to Riley the information that Hux had copied from Riley’s personal laptop after he was locked out of Hux’s office. This was the data that Hux had given to Gibbs & Bruns, the firm representing him in the Hospital Systems Solutions litigation. The Settlement Agreement does not cover materials placed on Hux’s computer (as opposed to Riley’s computer). The Settlement Agreement does not apply to materials and data that Hux could not have delivered to Gibbs & Bruns in 2002 because Riley alone knew of their existence.

Riley argues that the Settlement Agreement established a continuing duty on Hux to treat any information of Riley’s found on Hux’s computers—at any time—as confidential and give it to Gibbs & Bruns. This argument is unpersuasive. The relevant provision of the Settlement Agreement is written in the past tense. Hux agreed that all materials copied from Riley’s computers “*have been delivered* to Gibbs & Bruns and *have been designated* as Confidential Discovery Material.” Hux could only make that representation with respect to data he knew was in his possession. In 2002, when the Agreement was signed, Hux had no idea that *Riley* had copied information on to Hux’s hard drive. Hux could not have agreed that this information had *already* been delivered to Gibbs & Bruns and designated as confidential. That the Agreement creates continuing obligations does

not change this conclusion. The “Survival of Agreements” clause does not create new obligations; it requires Hux to continue complying with existing obligations. The Settlement Agreement did not require Hux to treat all information of Riley’s, no matter where or when it was found, as “Confidential Discovery Material” under the protective order.

Riley’s argument relies solely on the terms of the protective order and Settlement Agreement. Riley ignores the fact that he failed to take any steps to protect and retrieve the information he now asserts was protected as confidential under those documents. When Riley was negotiating for the return of the computers he had left in Hux’s office, and later for the copies Hux had made of information on those computers, he could have told Hux that he had stored information on one of Hux’s own computers and wanted this information returned to him. Riley could have arranged to have these files designated as Confidential Discovery Material under the protective order. *Cf. Bowles*, 224 F.R.D. at 257 (D.D.C. 2004) (holding that steps falling short of formal legal process were insufficient). Until sometime in 2004, Riley was the only person who knew that the information was on Hux’s computer. It was not reasonable for him to remain silent after he knew that others could gain access to those files.

The second factor is whether reasonably prompt action was taken to remedy the inadvertent disclosure. *See Alldread*, 988 F.2d at 1433-34 (citing *Hartford Fire Insurance*, 109 F.R.D. at 332). The evidence in this case shows that Riley failed to take any action for several years after he reasonably should have known that he had left confidential information on Hux’s computer and the password protection for that information had been removed. Riley was locked out of Hux’s office and learned that the network passwords had been compromised sometime in 2001. In 2004, Hux found the “Legal” directory Riley had stored on Hux’s computer and gave a copy to Alpert. In a hearing held in the probate court litigation on May 17, 2005, Riley sought to have the protective

order applied to the information contained in this directory. The record shows no action by Riley to retrieve the directory from Hux or to protect it from dissemination between 2001, when Riley reasonably knew that the directory was on Hux's computer without password protection, and May 2005, when the hearing occurred in the probate court. This delay is inconsistent with a desire to protect the confidential nature of the information on the directory. Riley waited much longer than the case law suggests is reasonable. *See, e.g., In re Grand Jury*, 138 F.3d at 981 ("While we cannot set an exact time within which such a motion must be made, we hold that the district court did not abuse its discretion in holding that Capano waived the privilege as we are satisfied that Capano acted unreasonably in waiting nearly four months to seek a judicial vindication of his assertion of the privilege."); *United States v. de la Jara*, 973 F.2d 746, 749-50 (9th Cir. 1992) (finding that the defendant's failure to act within six months of a letter's seizure by the government waived his attorney-client privilege); *Bowles*, 224 F.R.D. at 254-57 ("NAHB claimed privilege in correspondence with plaintiff but waited a year to take any legal action to assert its rights in the documents. This passivity is incompatible with plaintiff's obligation to 'jealously' protect any privilege in the documents."); *Apex Mun. Fund. v. N-Group Secs.*, 841 F. Supp. 1423, 1433 (S.D. Tex. 1993) ("Simply put, a one-year delay in taking any action to attempt to preserve the privilege exemplifies carelessness."); *Granada*, 844 S.W.2d at 227 (finding that waiver was supported by Granada's failure to remedy inadvertent disclosure within 11 months). Taking the first and second factors together, the record does not reveal any reasonable steps that Riley took to protect the confidentiality of his information within a reasonable amount of time.

Riley argues that in the May 2005 hearing, the state probate court judge stated that the Settlement Agreement and protective order covered the "Legal" directory files at issue. Riley argues that this statement is a ruling on the waiver issue that applies in this court. Texas preclusion law

applies to this question. 28 U.S.C. § 1738; *Lance v. Dennis*, 546 U.S. 459, 126 S.Ct. 1198 (2006); *Lange v. City of Batesville*, 160 Fed. App'x. 348, 351-52 (5th Cir. 2005) (per curiam) (unpublished). Under Texas law, “[a] party seeking to assert the bar of collateral estoppel must establish that (1) the facts sought to be litigated in the second action were fully and fairly litigated in the first action; (2) those facts were essential to the judgment in the first action; and (3) the parties were cast as adversaries in the first action.” *John G. & Marie Stella Kenedy Mem. Found. v. Dewhurst*, 90 S.W.3d 268, 288 (Tex. 2002). A careful review of the judge’s comments on the record in the probate court hearing show that he did not make a ruling with respect to waiver of privilege or work-product protection. The probate court judge did not make an express ruling as to whether Riley’s information left on Hux’s computer was covered by the protective order or that the order would apply to prevent waiver. The judge merely stated that the information on Hux’s hard drive was not discoverable from Hux because it was information that belonged to Riley. (Evidentiary Hearing Ex. 3 at 35-36). There was no ruling in the probate court that could have a preclusive effect on the waiver issue before this court.

The third factor, the scope of discovery, is not relevant. The inadvertent disclosure did not occur during discovery. The fourth factor is the extent of the disclosure. *Allread*, 988 F.2d at 1433-34 (citing *Hartford Fire Insurance*, 109 F.R.D. at 332). Disclosing a large amount of privileged information weighs in favor of finding waiver. *Hartford Fire Insurance*, 109 F.R.D. at 33. Jason Brodman testified that there were “tens of thousands” of files in the directory Riley placed on Hux’s computer. (Docket Entry No. 313 at 77). Riley has asserted a privilege over many of these documents, resulting in a privilege log with roughly 400 entries. Such a large disclosure is further support for a waiver finding.

The final factor, overriding fairness, does not warrant a different result. There is no evidence in the record that Hux acted improperly with respect to the data Riley placed on his computer. Once Brodman discovered the data, Hux sought the advice of counsel, who advised that the data was not subject to the protective order. There is no evidence that Hux hacked into the hard drive to obtain the data. Brodman testified that the information was not marked as privileged or confidential. And Riley had never told Hux that there was privileged or confidential material on Hux's own computer.

Considered together, the factors identified in the case law firmly support the conclusion that Riley waived his claims of attorney-client privilege and work-product protection for the directory and files he placed on Hux's computer.

IV. Conclusion

Riley has waived his claims of attorney-client privilege and work-product protection over the information he placed on Hux's computer.³

SIGNED on April 19, 2010, at Houston, Texas.



Lee H. Rosenthal
United States District Judge

³ The parties have also asked for clarification of a ruling on the record at the February 1, 2010 hearing. In discussing Riley's delay in producing documents and updating interrogatory answers, and ordering Riley to do so promptly, this court stated: "But I want to emphasize that this delay waives objections as to the information that we have gone over and that everything that has been requested in these categories must be produced." (Docket Entry No. 305 at 11). This ruling does not mean that Riley's existing objections, such as the privilege objections in his privilege logs, are waived. It means that he may not raise *new* objections relating to the information he had delayed in producing.